WHITEPAPER

DIGITALE DAADKRACHT

CYBEROPERATIES IN 2035

TNO innovation for life

Wat zou Defensie in 2035 aan **cybercapaciteiten** in huis moeten hebben, als niet al te grote maar **technologisch hoogwaardige krijgsmacht**? Hoe versterkt Defensie zijn 'digitale pantser', 'digitale slagkracht' en voorzettingsvermogen in cyberspace en het bredere informatiedomein? We kunnen ervan uitgaan dat in 2035 vrijwel álle inzetbare capaciteiten volledig zijn opgebouwd rond **digitale technologie**, bijvoorbeeld sensor-, wapen- en commando-voeringssystemen of logistiek. Deze afhankelijkheid brengt kwetsbaarheden met zich mee voor het militair optreden, omdat cyberspace een permanente contested environment is, waarin digitale dreigingen tegen defensiesystemen voortdurend bestaan. Het opbouwen van de cyber-capaciteiten van de toekomst begint dan ook met bescherming, een digitaal pantser dat weerbaarheid biedt tegen geavanceerde cyberaanvallen.

Verder heeft Defensie baat bij **slagkracht in het cyber-domein**, bij een eigen volwaardige offensieve cybercapaciteit voor militaire operaties, geïntegreerd in andere capaciteiten, waaronder informatie operaties. Tot slot is aandacht nodig voor het **voortzettingsvermogen in cyberspace**. TNO werkt deze visie in dit paper verder uit. We schetsen een **toekomstbeeld van de methoden en capaciteiten** die de digitale daadkracht van Defensie kunnen vormgeven, van offensieve en defensieve CEMA-capaciteiten[1] tot automatisering van cybersecurity-processen, en van geavanceerde monitoring en detectie voor het operationele domein tot toepassing van quantum-technologie en ontwikkeling van de cyberworkforce.

1 CEMA = Cyber and Electromagnetic Activities, een term waarmee de combinatie van cyber warfare en de (meer traditionele) elektronische oorlogsvoering wordt aangeduid.

Willen we dit realiseren, dan is het essentieel om samen te werken aan structurele ontwikkelpaden voor de zorgvuldig te kiezen onderwerpen: in een **‘gouden ecosysteem’** van Defensie, defensie- en cybersecurityindustrie en kennis-instellingen en zo mogelijk in internationaal verband. Deze zienswijze is TNO’s input voor een strategische dialoog over de opbouw van de geavanceerde Nederlandse cybercapaciteiten van de toekomst en gerichte deelname aan het European Defence Fund. We zetten de samenwerking in het ecosysteem graag verder op poten, onder regie van Defensie.

VOORWOORD

Cyberspace is na land, zee, lucht en de ruimte het vijfde operationele domein van de krijgsmacht. Ook hier treedt Defensie op om de veiligheid van Nederland te beschermen. Daarvoor ontwikkelt Defensie operationele cybercapaciteiten. Deze kunnen desgewenst ook worden ingezet als nichecapaciteit bij bondgenootschappelijk optreden. De huidige ambities van Defensie zijn momenteel vormgegeven in de Defensie Cyber Strategie (2018).

De Defensie Industrie Strategie (2018), die de ministeries van Defensie en Economische Zaken en Klimaat in 2018 publiceerden, merkte daarnaast het cyberdomein aan als gebied waarop Defensie over een sterke eigen kennispositie wil beschikken. Het beoogde profiel lijkt sterk op dat van het maritieme domein, waarin Defensie door sterke samenwerking in de ‘klassieke’ gouden driehoek met defensie-industrie en kennisinstellingen kan rekenen op eigen platforms en technologie van wereldniveau. Voor Nederland is dat succes ook in het cyberdomein bereikbaar, mits georganiseerd rondom een aantal speerpunten waarop ons land zelfvoorzienend of smart specifier wil zijn.

Dit paper beschrijft de visie van TNO op de ontwikkeling van cybercapaciteiten van de Nederlandse defensieorganisatie, binnen de context van het hele informatiedomein. Wat zou Defensie in de toekomst in huis moeten hebben als niet al te grote, maar technologisch hoogwaardige krijgsmacht? Ook de defensie- en cybersecurityindustrie moeten hier in een gouden ecosysteem bij worden betrokken.

Dit document is geen militaire cyberstrategie, maar een toekomstbeeld van methoden en capaciteiten die samen de digitale daadkracht van Defensie in 2035 zouden kunnen vormgeven: capaciteiten voor bescherming, slagkracht en voortzettingsvermogen in het cyberdomein. Dit beeld staat los van de organisatie, het juridische kader en de huidige situatie. Sommige ideeën zullen al bekend zijn of onderwerp van bestaand beleid of onderzoek zijn. Andere suggesties gaan juist verder dan wat nu al op de tekentafel ligt. We hebben gekozen voor 2035 als periode omdat dit een overzienbare periode is, die ook aansluit bij de huidige planningshorizon van Defensie.

Nieuw aan deze visie is de combinatie van alle inhoudelijke elementen én de realisatie ervan. Hierin is decennialange ervaring van TNO met opbouw van militaire cybercapaciteiten gevangen. Deze zienswijze is onze input voor een strategische discussie met Defensie, industrie en kennisinstellingen over de verdere ontwikkeling van de geavanceerde Nederlandse cybercapaciteiten van de toekomst.

INHOUDSOPGAVE

1. INLEIDING

In 2035 zijn vrijwel álle inzetbare capaciteiten van de krijgsmacht volledig opgebouwd rond geavanceerde digitale technologie. De sensoren, wapen- en commandosystemen (SEWACO) draaien op digitale technieken in een genetwerkte omgeving, binnen een 'system of systems'-benadering. De commandostructuur functioneert dankzij digitale technologie en logistieke, medische en andere ondersteunende capaciteiten kunnen alleen opereren door de inzet van informatietechnologie (IT).

Het voorzettingsvermogen in de toekomst is dus afhankelijk van de betrouwbaarheid van de digitale omgeving, met middelen die onderling steeds meer zijn verbonden. Denk aan zwermen van autonome systemen, *human enhancement,* geavanceerde sensoren, nieuwe adaptieve IT-netwerken, toepassingen voor *big data*-analyse en cloudvoorzieningen. Het onderscheid tussen binnen en buiten Defensie vervaagt verder door introductie van nieuwe IT-middelen. Ook doet quantumtechnologie haar intrede in het operationele domein, met kansen en bedreigingen voor het militair optreden.

Het waarborgen van het voortzettingsvermogen van de krijgsmacht, in een betwist digitaal domein *(contested cyber environment)*, wordt dan hoofdzaak. Dit in de wetenschap dat potentiële geavanceerde tegenstanders naar dominantie streven in het informatiedomein. Én dat minder ontwikkelde tegenstanders intensief gebruik zullen maken van asymmetrische tactieken om onze afhankelijkheid van het digitale en bredere informatiedomein uit te buiten. Defensie streeft ernaar altijd controle te houden over de eigen systemen en zelfstandig te kunnen handelen om het voorzettingsvermogen van de krijgsmacht te waarborgen. Wat is hier, onder die omstandigheden, voor nodig?

Afbakening van cyber
Afbakening van wat cyberspace wel en niet is wordt steeds minder relevant. Het draait in 2035 om het geïntegreerd beheersen en benutten van het informatiedomein, waarbij cyberoperaties een essentieel onderdeel zijn. Zo kan Defensie cybercapaciteiten inzetten tegen overwicht van tegenstanders in het fysieke of informatiedomein, als inlichtingenmiddel en als instrument voor de eigen weerbaarheid. Hoe de afbakening van cyber ook zal uitpakken: defensieve en offensieve cyberactiviteiten kunnen niet zonder een sterke *all-source* inlichtingen- en informatiepositie. Innovatie op de snijvlakken zorgt nu al voor nieuwe mogelijkheden, zoals draadloze aanvalsmethoden voor cyberaanvallen. Hier gaan we in de toekomst meer van zien.

FUNCTIES VAN OPERATIONELE CYBERCAPACITEITEN ONTWIKKELEN

In dit paper leggen we de digitale daadkracht of inzetbaarheid van Defensie uit op basis van een drietal functies van militair optreden, te weten bescherming, slagkracht en voortzettingsvermogen. We hebben ons hier laten inspireren door de joint functions uit de NAVO *Allied Joint Doctrine* (AJP-01) De overige functies die de AJP-01 onderscheidt, worden niet afzonderlijk behandeld, maar zijn (hier en daar) verweven in deze drie onderwerpen.

De functie bescherming noemen we hier ‘digitaal pantser’ en houdt de weerbaarheid in van systemen en netwerken tegen cyberaanvallen en cyber-incidenten.
‘Digitale slagkracht’ ziet op offensieve vermogens in cyberspace, van verkenning en inlichtingen tot het toebrengen van effecten. Het voorzettingsvermogen bestrijkt het aanpassingsvermogen van Defensie om mee te bewegen met de ontwikkelingen in het cyberdomein. Voor deze drie functies geven we een aantal technologieën weer, die bijdragen aan de digitale daadkracht van Defensie in 2035.

DE UITDAGING VRAAGT OM DUIDELIJKE KEUZES EN SAMENWERKING

Al met al ligt er een forse uitdaging. Als klein land willen we slim omgaan met de schaarse mensen, middelen, kennis en technologie. Dat vraagt om duidelijke keuzes tussen wat Defensie zelf ontwikkelt, waarvoor zij *smart specifier* wil zijn en waarvoor zij ‘slechts’ *smart buyer* is. Hetzelfde geldt voor de vraag wanneer nationale autonomie de boventoon moet voeren en wanneer we in Europees of ander internationaal verband optrekken. Het zal leiden tot een inzet van een mix van standaardmiddelen die ook civiel worden toegepast (COTS[2]), militaire standaardoplossingen (MOTS)[3] én maatwerk.

Samenwerking in het gouden ecosysteem, met kennisinstellingen en industrie is in elk van de opties van deze mix in enige mate nodig. Duidelijke roadmaps, of ontwikkelpaden, laten alle partijen het perspectief zien waarop zij kunnen inspelen.

LEESWIJZER

Het document is verder als volgt opgebouwd. Allereerst werken we het ‘wat’ uit: digitaal pantser (hoofdstuk 2), digitale slagkracht (hoofdstuk 3) en voortzettingsvermogen (hoofdstuk 4). Deze leiden in hoofdstuk 5 tot een conclusie. Tot slot nemen we u mee in de volgende stappen om te werken aan de digitale daadkracht van Defensie (aanbevelingen, hoofdstuk 6).

2 COTS = Commercial Off The Shelf
3 MOTS = Military Off The Shelf

2. BESCHERMING: HET DIGITALE PANTSER

Digitale inzetbaarheid begint met het weerbaar zijn tegen cyberaanvallen. Voor Defensie zullen die dreigingen uiteenlopen van een eenvoudige hack door een script kiddy tot een geavanceerde geïntegreerde en langdurige cyberoperatie door een (statelijke) actor.

In dit hoofdstuk werken we langs de as van de veiligheidsketen defensieve technologische ontwikkelingen uit: voor preventie, detectie en respons en herstel. Maar eerst benoemen we de aspecten van het digitaal pantser, zoals we die hier hanteren.

Ten eerste gaat het om het beheersen van digitale weerbaarheid en dus inzetbaarheid van SEWACO-systemen over de hele levenscyclus. In 2035 heeft Defensie dit van de eerste behoeftestelling tot en met de afstoting onder controle. Ten tweede overziet zij ook de leveringsketen of supply chain van de belangrijkste wapenplatforms.
Welke IT-componenten zitten erin, waar komen die vandaan en waar zitten de risico's? Op cruciale componenten is Nederland (of Europa?) inmiddels zelfvoorzienend: strategische digitale autonomie.

De derde invalshoek is de al genoemde veiligheidsketen, zoals die in de cybersecurity discipline veel wordt gehanteerd. Ten slotte gaat het bij het waarborgen van de digitale weerbaarheid om de bij beveiliging bekende trits beschikbaarheid, integriteit en vertrouwelijkheid.

PREVENTIE: ACTUEEL INZICHT IN CYBERRISICO'S

Een duidelijk en actueel inzicht in de cyberrisico's van de belangrijkste systemen en netwerken stelt Defensie in staat om gefundeerd besluiten te nemen over aanvullende maatregelen. Het geeft operationele commandanten ook inzicht in de inzetbaarheid van hun systemen. Dit is in 2035 een vanzelfsprekend onderdeel van Informatie Gestuurd Optreden in alle domeinen.

Zo weet Defensie in 2035 gedetailleerd welke digitale dreigingen relevant kunnen worden voor elk van de eigen systemen en is er omgekeerd een concreet beeld van relevante doelsystemen bij de tegenstander. Waar mogelijk wordt intensief samengewerkt met bondgenoten.

Defensie heeft ook een actueel inzicht in de status van haar eigen IT-omgevingen, zowel over het gehele Defensieapparaat als op het niveau van de operationeel commandant. Denk aan een in hoge mate geautomatiseerde *tactical decision aid*-cybertool die de commandant ondersteunt bij de *situational awarenes*s op IT-gebied. Ook afhankelijkheden van (systemen van) derden zijn helder en daarover zijn afspraken gemaakt met die derde partijen.

PREVENTIE: AUTOMATISERING EN KUNSTMATIGE INTELLIGENTIE

Preventie vereist kennis van welke IT-componenten in welke versie in huis zijn en welke kwetsbaarheden die bevatten. Dat maakt in elk geval IT-beheer en -onderhoud gemakkelijker en zorgt ervoor dat Defensie minder tijd verliest bij cyberaanvallen.

IT-componenten worden bij opstarten, maar ook gedurende het gebruik, automatisch gecontroleerd op integriteit. Hetzelfde geldt voor componenten die voor onderhoud uit het platform zijn verwijderd en weer worden teruggebracht. Voor de meest kritieke toepassingen kan de integriteit zelfs op chipniveau worden gegarandeerd door gebruikmaking van speciale lithografietechnieken. Cybersecurity vindt steeds meer plaats op chipniveau.

Omdat handmatig zoeken naar kwetsbaarheden in alle systemen ondoenlijk is, worden meerdere technieken ingezet, zoals kunstmatige intelligentie, om kwetsbaarheden op te sporen en zo veel mogelijk automatisch te patchen. Deze kennis is overigens ook offensief in te zetten.

In een operationele omgeving vinden op alle systemen periodieke testen op weerbaarheid plaats. Deze zijn grotendeels geautomatiseerd om mensen en middelen te besparen. Ook binnen reguliere oefeningen vinden, binnen veiligheidsmarges, live dergelijke testen plaats op systemen, geïnspireerd door eerdere vergelijkbare programma's in de vitale sectoren (bijvoorbeeld het TIBER programma in de bankensector).

PREVENTIE: MENSEN BLIJVEN EEN ESSENTIËLE SCHAKEL

Mensen, of het nu medewerkers, leveranciers of derden zijn, vormen een belangrijke schakel in het voorkomen van incidenten en veilig houden van systemen. Dat vergt een ander soort bewustzijn. De vertaling naar digitaal veilig gedrag is cruciaal, en kan deels door de organisatie worden gefaciliteerd. Doel is dat medewerkers (en leveranciers) hun werkzaamheden eenvoudig en veilig kunnen uitvoeren met de middelen en ondersteuning die daarbij horen.

Door voldoende werkende voorzieningen voor op zichzelf logische handelingen op de werkplek aan te bieden, wordt het voor personeel steeds gemakkelijker zich veilig te gedragen. Zo wordt bijvoorbeeld het op een veilige manier verwerken en gebruiken van verschillend gerubriceerde data gefaciliteerd. Of door automatisch labelen van (delen van) data en op risicoprofielen gebaseerde toegang moet het weer gemakkelijker worden om veilig te handelen dan onveilig en Informatie Gestuurd Optreden te faciliteren zonder additionele cyberrisico’s.

De zichtbaarheid in het elektromagnetisch spectrum van elk IT-apparaat, of het nu gaat om een slim soldatenpak of een netwerk, leidt in 2035 tot inzet van diverse concepten en hoogwaardige en *lowtech* technieken voor digitale camouflage. Zo voorkomt Defensie dat tegenstanders die gebruikmaken van CEMA-middelen de locatie en identiteit van troepen op een bruikbare manier in kaart kunnen brengen. Dit vergroot de overlevingskansen: uiteindelijk dient cybersecurity de veiligheid van mensen.

PREVENTIE: TOEKOMSTBESTENDIGE CRYPTO

Het is niet denkbeeldig dat in 2035 de quantumcomputer in staat is razendsnel sommige vormen van crypto te breken. Dit geldt in het bijzonder voor asymmetrische crypto, waarbij de gebruiker twee verschillende sleutels nodig heeft voor versleuteling en ontgrendeling. Deze methode wordt in veel digitale communicatiemiddelen toegepast.

Defensie heeft voor haar cryptovoorzieningen dus een weerwoord op de toekomstige kracht van de quantumcomputer nodig. Inzicht in relevante technologie en tijdige maatregelen door het Ministerie van Defensie en de defensie-industrie hebben dat tegen die tijd mogelijk gemaakt. Omgekeerd kan quantumtechnologie cybersecurity technologie ook verbeteren, b.v. door quantum algoritmes in te zetten bij monitoring & detectie of in het algemeen sneller AI algoritmes te laten leren.

Quantum-safe of niet, crypto moet ook in 2035 beschermen tegen afluisteren, maar mag samenwerking met bondgenoten niet teveel in de weg staan. Voor veilige tactische communicatie ‘in het veld’ is daarom interoperabiliteit van tactische crypto een operationeel vereiste . Nederland beschikt als één van een beperkte groep Europese landen over een gedegen cryptokennis en -industrie om dit te helpen opbouwen.

DETECTIE: DREIGINGEN ZO VROEG MOGELIJK ONDERKENNEN

Onderdeel van het actuele inzicht in cyberrisico’s is het kunnen monitoren van alle transmissiekanalen, netwerken- en systemen in onderlinge samenhang voor het zoeken naar dreigingen in het informatiedomein. In 2035 is veel voortgang geboekt in het terugdringen van de gemiddelde detectietijd door de inzet van monitoring- en detectietechnologie.

Dit begint met het real time kunnen monitoren van álle systemen en het onderling (en over de tijd heen) kunnen correleren van gegevens die daaruit voortvloeien. Zowel de operationele als bestuurlijke IT-systemen beschikken daarom over de mogelijkheid om relevante data real time veilig af te staan aan monitoringsystemen. Zowel lokaal als centraal is er een actueel situatiebeeld. Defensie beschikt in 2035 ook in het operationele domein over voldoende connectiviteit en bandbreedte om die informatie van alle systemen te verzamelen en te verspreiden[4].

4 In tegenstelling tot het civiele domein is de beperkte beschikbaarheid van connectiviteit en bandbreedte in het operationele domein op dit moment nog steeds een grote hindernis bij het optimaal benutten van de mogelijkheden van digitalisering. Dat geldt ook voor de in dit paper beschreven cybercapaciteiten.

Cyberexperts kunnen zowel de inrichting met zoekalgoritmes als de configuratie van hun technische detectieplatformen ad hoc naar bevind van zaken aanpassen. Dit zorgt ervoor dat aanvallers van tevoren niet betrouwbaar kunnen testen of hun aanval ongemerkt door de detectie heen kan komen, zelfs niet als ze door verkenning weten wat Defensie aan defensieve technologie in huis heeft. De aanvaller moet rekeninghouden met allerlei opties, net als de verdedigende partij dat met aanvallers moet doen.

Incidenten worden zoveel mogelijk al aan de voorkant opgevangen, bij de systemen zelf. Detectiealgoritmes kijken daar al naar alarmerende afwijkingen en informeren zo nodig de gebruiker en beheerder. Dat moet wel op maat gebeuren: aan boord van een pantservoertuig is er nu eenmaal minder handelingsperspectief dan aan boord van een groot schip.

Voor het lokaal detecteren van CEMA-aanvallen in het veld rust Defensie haar teams uit met kleine sensoren, die waarschuwen wanneer een tegenstander zo'n middel inzet, bijvoorbeeld om vast te stellen wanneer die tegenstander probeert de unieke identiteit van een mobiel apparaat én persoon te achterhalen of aan te vallen. Dat laatste zal door het stijgende gebruik van steeds kleinere maar krachtige persoonlijke digitale apparaten steeds belangrijker worden.

RESPONSE EN HERSTEL: DEFENSIEF MANOEUVREREN IN HET CYBERDOMEIN

De laatste twee onderdelen van de veiligheidsketen zijn response en herstel; zij zijn beide belangrijk voor het kunnen blijven uitvoeren van missies en de reguliere bedrijfsvoering. Hoe minder hinder missies ondervinden van cyberincidenten, hoe beter. Zoals gezegd is onverstoorde beschikbaarheid daarvoor cruciaal. Als dat niet mogelijk is, zal een systeem door middel van *graceful degradation* de gebruikers moeten kunnen blijven bedienen van de meest essentiële functies. Desnoods met niet-digitale opties: analoog of met fysieke hendels en knoppen!

Naast het terugdringen van de gemiddelde detectietijd is ook het versnellen van de response dus belangrijk om het voortzettingsvermogen van Defensie te versterken. Omdat de tijd om te reageren kort is, zijn in 2035 meerdere responseprocessen geautomatiseerd. Bijvoorbeeld door inzet van *playbooks* die systemen of gebruikers handmatig kunnen inschakelen om geautomatiseerd de noodzakelijke cybersecurityprocessen uit te voeren.

De *tactical decision aid* cyber speelt een belangrijke rol bij het deel waar de mens moet ingrijpen: het geeft de gebruiker de noodzakelijke informatie over het incident en de opties om daarop te acteren, het handelingsperspectief. Een aandachtspunt is het risico van informatie-overload bij gebruikers onder gevechts- of oefenomstandigheden. Zo veel mogelijk wordt daarom automatisch afgehandeld. Het toekomstbeeld wordt gevormd door de *self healing* systemen die zelf zorgen dat kwetsbaarheden en aanvallen worden weggewerkt, zonder dat de gebruiker hoeft in te grijpen.

Technologie helpt om het voordeel dat de aanvaller heeft ten opzichte van de verdediger te verkleinen. Defensie kan in 2035 ook in defensief oogpunt manoeuvreren in het cyberdomein. De netwerken van de nieuwe SEWACO-systemen zijn dynamisch ingericht door software-gedefinieerde technologie (*software defined networks*). Bij een aanval kunnen componenten in het netwerk zich zelfstandig anders inrichten (*morphing*), zodat het voor de aanvallende partij minder duidelijk wordt waar hij zich bevindt in het netwerk of waar de digitale kroonjuwelen zich bevinden. Ook door toepassing van andere misleidende technologieën als obfuscatie (versluiering), encryptie en *honey pots* worden aanvallers voortdurend op het verkeerde been gezet.

In dit hoofdstuk hebben we een aantal technologische ontwikkelingen de revue laten passeren die het digitaal pantser van Defensie kunnen versterken. Niet alleen de aanvallers zijn innovatief, de digitale verdediging is dat ook. De balans gaat hier al met al verschuiven van reageren op incidenten naar proactief voorspellen en automatisch opvangen van toekomstige problemen.

3. SLAGKRACHT IN HET CYBERDOMEIN

Defensie heeft baat bij een eigen volwaardige offensieve cybercapaciteit bij het uitvoeren van militaire operaties. Daarmee kan zij op diverse niveaus effecten teweegbrengen. In 2035 is cyber daarom één van de vele inzetopties, ofwel ‘just another tool in the toolbox’ van de commandant.

Zoals Defensie op dit moment genietroepen, helikopters en inlichtingencapaciteit aan een missie toebedeelt, maakt cyber in 2035 integraal deel uit van militaire operaties. Het is een logisch middel dat in samenhang met o.a. elektronische oorlogsvoering en *communication & engagement* wordt betrokken bij militaire besluitvormingsprocessen. In dit hoofdstuk volgen we de indeling van besluitvorming, ontwikkeling van een inzetbaar middel en de daadwerkelijke inzet van cybermiddelen.

BESLUITVORMING: INFORMATIE GESTUURD OPTREDEN EN HET CYBERDOMEIN

In 2035 neemt de operationele staf zowel defensieve als offensieve cyberaspecten mee in besluitvormingsprocessen. Welk effect moet worden bereikt, welke middelen kunnen daartoe worden ingezet en wat is de dreiging en de mogelijke response van de tegenstander? Uiteraard past dit binnen een up-to-date cyberdoctrine, die ook richtinggevend is voor de doorontwikkeling van cybercapaciteiten en integratie met andere domeinen, waaronder het informatiedomein.

De commandant en diens staf maken gebruik van geautomatiseerde ondersteuning voor besluitvormingsprocessen, die hen helpen bij het modelleren, doorrekenen en kwantificeren van verschillende opties en mogelijke effecten. Een offensieve *tactical decision aid cyber* dus.

In 2035 is het personeel getraind in welke effecten op zowel de fysieke als de mentale component van de tegenstander met cyber- (of andere informatie-) middelen kunnen worden bereikt.

Aangrijpen van de fysieke component kan inhouden het uitschakelen van de SEWACO-systemen van de tegenstander. Bijvoorbeeld een cruciale schakel in een gedistribueerd luchtafweersysteem, zodat de luchtmacht met minder gevaar een actie kan uitvoeren. Ook bij de tegenstander zijn transmissiemiddelen belangrijke schakels en dus een interessant aangrijpingspunt. Weten welke schakels dat zijn en hoe die qua IT zijn opgebouwd is cruciale informatie.

Voor wat betreft de mentale component van de tegenstander kan de inzet zijn gericht op het manipuleren van informatie of informatiesystemen en daarmee het aantasten van de gevechtsbereidheid van de vijand en het moreel van de bevolking. Of denk aan irreguliere oorlogvoering via sociale media of andere digitale kanalen.

Specifieke aandacht is er ook voor mogelijke nevenschade, omdat cybermiddelen een groot bereik van bedoelde of onbedoelde schade kunnen hebben. Om diens besluitvorming te ondersteunen heeft de operationeel commandant ook daarvoor analysetools voorhanden, die hem helpen de juiste inschatting te maken.

ONTWIKKELING: GEÏNDUSTRIALISEERDE WERKWIJZE DRAAGT BIJ AAN KWALITEIT

In sommige gevallen is een klein team van slimme cyberoperators voldoende voor een geslaagde operatie. Maar geavanceerde operaties gaan de komende jaren steeds meer lijken op het geïndustrialiseerd bouwen en onderhouden van ‘gewone’ software. De experts werken gedurende langere tijd binnen een specifieke architectuur, met standaard werkprocessen en tools, AI en met modules om de verschillende stappen in de *cyber kill chain* (of *attack flow*) te kunnen maken, vergelijkbaar met het plotten van soorten operaties in een klassiek geweldspectrum.

Het voordeel van de geïndustrialiseerde methode schuilt onder andere in continuïteit, efficiëntie, minder afhankelijk zijn van individuen, risicoreductie bij planning en uitvoering en controleerbaarheid van de inzet van cyberwapens achteraf.

Defensie beschikt in 2035 over een afgeschermde ontwikkelomgeving van wereldklasse met gestandaardiseerde processen, ondersteunende tools en mechanismen voor kwaliteitsbewaking, testen en configuratiebeheer. Binnen die ontwikkelomgeving creëren cyberteams op creatieve en effectieve wijze de voor de operatie benodigde middelen. Hergebruik van componenten wordt gefaciliteerd en databases met kwetsbaarheden, *exploits*, tools, enzovoorts worden bij elkaar gebracht. Deze standaarden waarborgen traceerbare kwaliteit en continuïteit, alsmede kennismanagement.

Die operationele middelen kunnen zich bijvoorbeeld richten op *command & control* van het cyberwapen, obfuscatietechnieken (versluiering) en encryptie. Maar ook op de *payloads*, de effectbrengers zelf, hoewel dat vaak maatwerk zal zijn.

Om relevant te blijven in de dynamiek van technologische ontwikkelingen worden de middelen voortdurend onderhouden om de effectiviteit zo goed mogelijk te kunnen borgen.

Automatisering en kunstmatige intelligentie kunnen deze geïndustrialiseerde methode verder ondersteunen. Defensieve technieken om automatisch kwetsbaarheden te vinden op eigen systemen kunnen ook op die van tegenstanders worden toegepast, en daarna worden omgezet in *exploits*, code om de kwetsbaarheden te misbruiken. Deze toepassing zal duidelijke, gebalanceerde regulering moeten krijgen, omdat die kwetsbaarheden systemen kunnen betreffen die (vitale) organisaties en burgers in Nederland zelf ook gebruiken.

INZET: TACTISCHE CYBERMIDDELEN ONDERSTEUNEN MILITAIRE OPERATIES

Naast capaciteiten voor strategische operaties, beschikt Defensie in 2035 over mobiele tactische middelen ter ondersteuning van militaire operaties in het veld, ter zee of in de lucht. Bij tactische middelen gaat het om relatief eenvoudige, draagbare tools die met minder specialistische kennis in het veld (of zee of lucht) kunnen worden ingezet om lokaal effecten te bereiken of om meer strategische operaties te ondersteunen.

Een voorbeeld is een modulair platform dat militairen de mogelijkheid biedt om een goed situatiebeeld op te bouwen over het lokale gebruik van civiele en militaire communicatiekanalen en de aanwezigheid van apparaten in de nabijheid.
Om negatieve neveneffecten van kinetische operaties te beperken, is ook denkbaar dat Defensie tactische CEMA-middelen inzet om van een afstand of van dichtbij de digitale middelen van tegenstanders in kaart te brengen en/of lokaal aan te grijpen.

Ook voor de ontwikkeling en beheer van tactische cyberwapens geldt dat er veel overeenkomsten zijn met ‘gewone’ IT. Door te leren van de werkwijze van de commerciële IT-wereld en die van de elektronische oorlogsvoering, werken Defensie en haar partners efficiënt toe naar onderhoudbare *joint* oplossingen voor mobiele tactische cybermiddelen.

Hoewel de nadruk in dit hoofdstuk lag op offensieve cyber op het tactische niveau, zijn dezelfde methoden en technieken ook onverminderd van toepassing bij een strategische inzet van het cyberwapen.

In dit hoofdstuk hebben we verschillende aspecten van offensief optreden in het cyberdomein bekeken. Van informatiegestuurde besluitvorming tot inzet van cyber- en CEMA-middelen tijdens operaties. De veelzijdigheid van bereikbare effecten en inzetmogelijkheden noodzaken tot een meer industriële benadering van gereedstelling van cybermiddelen. Maatwerk voor elk cybermiddel (of effect) is praktisch en financieel gezien onhaalbaar.

4. VOORTZETTINGSVERMOGEN IN CYBERSPACE

Pantser en slagkracht bestaan alleen zolang Defensie ook voortzettingsvermogen heeft, zich kan blijven aanpassen aan veranderende omstandigheden. Dat bestaat uit operationeel, technologisch en organisatorisch aanpassingsvermogen. Samenwerking in het gouden ecosysteem versterkt deze vermogens.

OPERATIONEEL AANPASSINGSVERMOGEN: AANBESTEDING VAN MATERIEEL ALS STARTPUNT

De nieuwste wapenplatforms waarover Defensie in 2035 beschikt, zijn fundamenteel flexibel. In plaats van een meer rigide opbouw, zoals een wapensysteem dat straks draait op Windows 10 terwijl die versie twintig jaar later niet meer bestaat, bewegen de platforms gemakkelijk en betaalbaar mee met veranderende omstandigheden.

Flexibiliteit start bij het begin van de levenscyclus van systemen en netwerken. Dat is mogelijk door die eigenschap bewust al mee te nemen in behoeftestelling, ontwerp en architectuur, en aanbesteding en contractering. Vanuit defensief oogpunt is dat essentieel. Het aanschaftraject van een fregat of vliegtuig duurt vele jaren. Die tijd is nodig, maar tegelijk zullen de hardware en software snel verouderen.

Defensie is in 2035 in staat tijdig alle software en hardware van SEWACO-systemen en ondersteunende processen aan te blijven passen om de beveiliging en beschikbaarheid te kunnen waarborgen. Zij moet altijd kunnen beschikken over de meest recente software versies die het minst kwetsbaar zijn voor aanvallen van buitenaf en regelmatig een beveiligingsupdate ontvangen.

ORGANISATORISCH VERMOGEN: ONTWIKKELING VAN DE CYBERWORKFORCE

Het opbouwen van een cyberworkforce kost jaren. Daar komt bij dat cyberkennis dynamisch is en we als klein land allemaal uit dezelfde vijver vissen met een schaarste aan de juiste experts. Ontwikkeling van een cyberworkforce vraagt dus aanpassingsvermogen van de defensieorganisatie, intern en in relatie tot diens omgeving.

Het wordt verder steeds belangrijker dat alle militairen enige mate van cyberkennis bezitten. De gebruiker van een wapen met een digitaal onderdeel hoeft niet een hack te kunnen oplossen, maar hij moet deze wel herkennen om de juiste informatie te kunnen doorgeven bij een incidentmelding. De staf van een operationeel commandant moet kunnen adviseren over de cyberrisico's voor inzetbaarheid of de aantrekkelijkheid van cyberopties om operationele effecten te bereiken.

Mede door de schaarste aan experts is het noodzakelijk om iedereen die de ambitie heeft om bij Defensie een carrière op te bouwen daadwerkelijk in te zetten, van mbo'er en hbo'er tot wo'er. Samenwerking in het gouden ecosysteem draagt extra bij aan het vinden en binden van zulk geschoold personeel.

Ook het bieden van loopbaanperspectief en gerichte ontwikkeling van professionals zijn belangrijke randvoorwaarden om optimaal rendement uit dit schaarse middel te halen. Met carrièrepaden binnen en buiten Defensie, waarbij mensen steeds de werkplek vinden die op dat moment bij ze past, draagt de organisatie samen met de industrie en kennisinstellingen bij aan een leven lang ontwikkelen.

ORGANISATORISCH AANPASSINGSVERMOGEN: REALISTISCHE TRAININGEN EN OEFENINGEN

Een ander belangrijk aandachtspunt zijn de kennis en vaardigheden van medewerkers. Defensie weet experts aan zich te binden door ze in een realistische omgeving te laten trainen, zoals door een investering in virtuele en fysieke omgevingen waar realistische scenario's worden uitgevoerd. Daarbij past ook het uitwisselen met andere overheidsorganisaties zoals de inlichtingendiensten en de Nationale Politie, waar de experts hun vaardigheden met *train as you fight* ontwikkelen en onderhouden.

Zeker omdat er steeds nieuwe onderwerpen en kwetsbaarheden zijn waarmee militairen moeten leren omgaan, zijn sterke en uitdagende simulatiemiddelen voor training en opleiding een absolute must. In 2035 beschikt Defensie over voldoende en realistische mogelijkheden voor alle soorten cyberprofessionals. Zo kennen alle oefeningen standaard een cybercomponent, die bij voorkeur live wordt uitgevoerd. Verder zijn cybereffecten en bijbehorende neveneffecten ook in de reguliere simulatieomgevingen gemodelleerd, waar cyberoperators in sommige gevallen kunnen meetrainen. Dat geldt ook voor oefeningen, waarin nationaal of met bondgenoten cybereffecten worden ingebracht, of soms zelfs live op deelnemers aan de oefening.

Voor geavanceerde defensieve trainingen en bij het testen van nieuwe technologie gebruikt de krijgsmacht *digital twins*: digitale modellen van majeure wapenplatforms, waarin de meest representatieve systemen en netwerken zijn vormgegeven. Deze digital twins zijn ook te gebruiken voor testen van technische patches en updates.

Verder werkt Defensie op het gebied van defensieve training meer samen met andere Europese landen, onder meer omdat toekomstige operaties in de regel plaatsvinden in internationale context en omdat trainingsbehoeftes grotendeels overeenkomen. Wat dat betreft hebben de initiatieven tot meer Europese samenwerking in cyber-opleiding en training bij de European Defence Agency (EDA) en via de Permanent Structured Cooperation (PESCO) hun vruchten afgeworpen. Na aanvankelijke voorzichtigheid worden ook offensieve trainingen en oefeningen internationaal aangevlogen met een selecte groep bondgenoten.

Nederland zal nooit over een even omvangrijke cyberworkforce kunnen beschikken zoals die van grootmachten, dus moet ons land slim om gaan met capaciteit. Naast reservisten kan Defensie, zoals ook nu al het geval is, bij crisis een beroep doen op expertise die bij de industrie of een overheidsorganisatie is belegd. Omdat in een toekomstig conflict ook civiele organisaties doelwit kunnen zijn van cyberaanvallen, is voor experts een helder prioriteringsmechanisme bedacht op nationaal niveau.

TECHNOLOGISCH AANPASSINGSVERMOGEN: FOCUS, REGIE EN SAMENWERKING

Naast operationeel en organisatorisch vermogen is ook technologisch aanpassingsvermogen van de Defensieorganisatie van belang. De mate tot technologische vernieuwing en vermogen tot aanpassing gaat gelijk op met het vermogen van Defensie om nieuwe ontwikkelingen te absorberen. Dit is voor cyber niet anders dan voor andere kennisgebieden. Gegeven de blijvende schaarste aan cyberexpertise is dat absorptievermogen echter eindig. Door het aanbrengen van inhoudelijke focus is er meer tijd en ruimte om regie te voeren op onderhoud en vernieuwing van capaciteiten. Operationele inzetscenario's in alle domeinen (land, zee, lucht, ruimte, cyber) zijn leidend bij het aanbrengen en behouden van focus.

Defensie voert regie op de ontwikkeling van capaciteiten. Uitgangspunt is het succesvolle model van samenwerking in het gouden ecosysteem van Defensie, defensie- en cybersecurityindustrie en kennisinstellingen. Defensie maakte daarbij duidelijke keuzes. Voor wat zij zelf doet, waar zij *smart specifier* is als opdrachtgever voor nieuwe of te onderhouden capaciteiten en voor waar zij 'alleen' *smart buyer* is van materialen van de plank.

Om niet te afhankelijk te zijn van leveranciers, beschikt Defensie, ondersteund door de kennisinstituten, als *smart buyer* over specialistische kennis om te weten wat de eisen zijn en hoe die te toetsen. Dit geldt zowel voor defensieve technologie als voor operationele capaciteiten.

Samenwerking met derden is gezien de snelheid van ontwikkelingen en beperkte eigen capaciteit een essentiële keuze. Het bedrijfsleven en kennisinstellingen nemen een deel van het volgen van die technische ontwikkelingen en het omzetten in capaciteiten voor Defensie voor hun rekening.

In dit hoofdstuk hebben we gekeken naar verschillende aspecten van het voorzettingsvermogen van Defensie als onderdeel van de digitale daadkracht. Flexibiliteit van materieel, de mens en technologisch aanpassingsvermogen zijn essentieel.

5. CONCLUSIE

De digitale inzetbaarheid van Defensie steunt op drie factoren: digitaal pantser, digitale slagkracht en voortzettingsvermogen in cyberspace. Voor het opbouwen van de cybercapaciteiten van de toekomst is er de komende vijftien jaar voor elk van die factoren werk aan de winkel, gefaciliteerd door samenwerking in het gouden ecosysteem van Defensie, defensie- en cybersecurityindustrie en kennisinstellingen.

Het informatiedomein beheersen en/of de tegenstander informatiedominantie kunnen ontzeggen, zijn belangrijke succesfactoren voor toekomstige conflicten. Defensieve en offensieve cyber operaties spelen hier een essentiële rol in en die kunnen alleen bestaan door voortzettingsvermogen in cyberspace. De grens van wat cyber is en wat niet, wordt hierbij steeds vager in de praktijk. Samenwerking tussen disciplines is daarom nodig, gericht op de gezamenlijk te bereiken effecten.

Kijkend naar digitaal pantser, digitale slagkracht en voorzettingsvermogen zien we een aantal rode draden. Zo worden in alle functies automatisering en toepassing van AI belangrijk om nieuwe capaciteiten te ontwikkelen en in te zetten. Zo ondervangt Defensie niet alleen de blijvende schaarste aan expertise, maar helpt het ook om een antwoord te hebben op de hoge dynamiek in cyberspace en de enorme hoeveelheden te verwerken data. Automatisering en AI zijn in defensief opzicht noodzakelijk om meer ‘*ahead of the curve*’ te komen: van reageren op incidenten naar proactief voorspellen en problemen oplossen voordat ze zich echt openbaren. Ook voor (voorbereiden van) offensief optreden bevorderen geautomatiseerde werkwijzen de effectiviteit, efficiëntie en controleerbaarheid achteraf.

Het digitaal pantser is anno 2035 afdoende tegen hoogwaardige statelijke actoren en dat vergt een integrale benadering die de hele levenscyclus van SEWACO-systemen en andere verbonden systemen en netwerken afdekt. Die integrale benadering is niet van de één op de andere dag gerealiseerd, want die is omvangrijk en bevat tal van organisatorische en technische uitdagingen. Het is hierbij continu zoeken naar de balans van digitale weerbaarheid met zaken als functionaliteit, financiën, informatiedeling en samenwerking.

Zowel defensief als offensief kan er voorts ook in cyberspace informatie gestuurd worden opgetreden. Dat is uiteraard geen doel op zich. Instrumenten als een *tactical decision aid cyber* helpen de militair aan meer informatie, inzicht en meer handelingsperspectief en bevorderen daarmee de overlevingskansen en voortzettingsvermogen van Defensie als geheel.

De mens blijft voorlopig ‘in the lead’. Sterker nog, de mens als professional, beslisser of gebruiker heeft een sleutelrol bij het voortzettingsvermogen in het cyberdomein en dat is niet vrijblijvend. Op elk niveau is cyberkennis nodig, en hoe realistischer oefeningen en trainingen zijn vorm gegeven, hoe beter de transitie naar de praktijk.

6. AANBEVELINGEN

De ontwikkelingen in het cyberdomein gaan razendsnel en de expertise is schaars. Het toenemende belang van cyber voor de veiligheid van Nederland en Defensie zelf maakt regie op ontwikkeling van cybercapaciteiten daarom broodnodig. Die regie betreft zowel de inhoudelijke visie als de organisatie van het proces van samenwerking en ontwikkeling.

Het technologisch aanpassingsvermogen is hier essentieel. Kan Defensie tijdig en voldoende richting geven aan de ontwikkeling van het digitale pantser, digitale slagkracht en het voortzettingsvermogen in cyberspace? We doen hieronder een aantal concrete aanbevelingen.

1. GERICHTE CAPACITEITSONTWIKKELING IS DE SLEUTEL TOT SUCCES

Capaciteitsontwikkeling rond de functies bescherming, slagkracht en voortzettingsvermogen kent een sterke onderlinge samenhang. Gezien de complexiteit van het domein en de structurele schaarste aan capaciteit en middelen, blijven consistente focus en samenwerking voor Defensie van essentieel belang: in de diverse internationale verbanden, maar ook in het gouden ecosysteem.

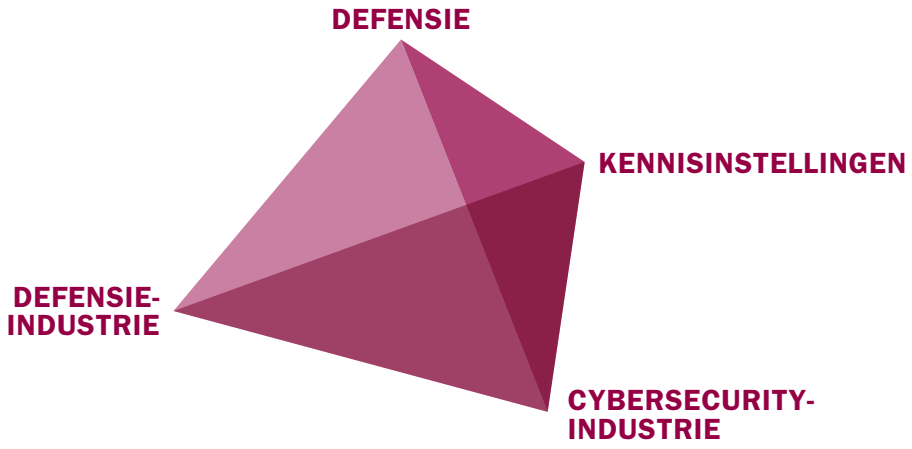
Zo denkt TNO aan gezamenlijke structurele ontwikkelpaden onder regie van Defensie voor o.a. de volgende onderwerpen:
– inzet van automatisering en AI in alle functies;
– informatiegestuurd optreden en het cyberdomein;
– integrale benadering digitaal pantser;
– cyberworkforce development.

Hierbij is het zaak de balans te houden tussen groot denken en klein beginnen en soms ook capaciteiten klein en eenvoudig te houden. Sneller beginnen met praktijkervaringen met beperkt opgezette middelen zorgt voor kortere feedback loops voor het hele ontwikkelpad. Zijn we op de goede weg? Werkt dit, of waarom niet? Wie kan dit een stap verder brengen? Quick wins zijn verder vaak op snijvlakken van verschillende disciplines te vinden. Deze benadering heeft synergie met het gestaag opbouwen en onderhouden van een gedegen kennisbasis op digitaal pantser, digitale slagkracht en voortzettingsvermogen voor vernieuwingen die een langere adem vergen.

2. DOOR STRATEGISCHE DIALOOG KOMEN WE TOT MEERJARIGE ONTWIKKELPADEN

Een interessante inspiratiebron voor cyber is het maritieme domein, waar samenwerking in de gouden driehoek van Defensie, defensie-industrie en kennisinstellingen al decennialang leidt tot wapenplatforms en technologie van wereldklasse. Defensie stelt de doelen (het 'waarom'), terwijl de uitwerking (het 'hoe' en 'wat') grotendeels plaatsvindt in de andere takken van het ecosysteem. Nederland Radarland is een voorbeeld. Dat is niet één op één te kopiëren voor cyber- of het informatiedomein, maar biedt wel veel lessen.

Vanuit die insteek start TNO graag een proces van strategische dialoog over de kennisvisie op cyber en de opbouw van de capaciteiten van de toekomst. Dat proces kunnen we vormgeven door samenwerking in het gouden ecosysteem, waar ook de industrie bij is aangesloten, langs meerjarige ontwikkelpaden die uiteindelijk zijn gekoppeld aan het Defensie Materieel Proces en de operationele inzetbaarheid.



Het gouden ecosysteem voor cyberoperaties van Defensie

3. REGIE DOOR DEFENSIE VOOR RICHTING EN SAMENHANG

Logischerwijze ligt de regie op de samenwerking en ontwikkelpaden bij Defensie. De behoeften van Defensie zijn immers richtinggevend. Dat wil niet zeggen dat ook alle uitvoeringslasten daar liggen. Die regierol is ook belangrijk om synergie te bewerkstelligen met aanpalende nationale speerpunten en inspanningen in internationaal verband, zoals de Kennis- en Innovatie Agenda's Veiligheid en Sleuteltechnologieën, de Nationale Cryptostrategie, Nationale AI Strategie, Nationale Agenda Quantum Technologie en het European Defence Fund. Defensie participeert al actief in al deze agenda's en kan de samenhang overzien.

Door als klein land slim om te gaan met schaarse personele capaciteit, financiële middelen, tijd, energie en aandacht komen we met elkaar tot één verhaal, één strategie en een veilig Nederland voor iedereen die hier wil wonen en werken. En tot een defensieorganisatie die ook in het toekomstige informatiedomein hoogwaardig opereert en Nederland én haar eigen mensen veilig houdt.

REFERENTIES

1. Algemene Rekenkamer, Digitalisering aan de grens. Cybersecurity van het grenstoezicht door de Koninklijke Marechaussee op Schiphol, 2020
2. Cheng, Dean, Cyber Dragon, 2019
3. De Nederlandsche Bank, TIBER-NL GUIDE, How to conduct the TIBER-NL test, 2017
4. Ducheine, Paul, Defensie in het digitale domein, Militaire Spectator, 2017
5. Fischerkeller, Michael P., Harknett Richard J., Deterrence is Not a Credible Strategy for Cyberspace, 2017
6. Geveke, Henk, Technologische revoluties en Defensie. De gevolgen van nieuwe technologische ontwikkelingen voor Defensie, Militaire Spectator, 2016
7. Hamilton, Stephen and Jan Kallberg, *Integrate cyber maintenance into the US Army's battle rhythm, Fifth Domain,* https://www.fifthdomain.com/show-reporter/ausa/2019/10/07/integrate-cyber-maintenance-into-the-us-armys-battle-rhythm, geraadpleegd op 1 maart 2020
8. Holland High Tech, Kennis- en Innovatie Agenda Sleuteltechnologieën, 2019
9. Maurer, Tim, Cyber Mercenaries. The State, Hackers and Power, 2018
10. Ministerie van Defensie, Defensie Cyber Strategie, 2018
11. Ministerie van Economische Zaken en Klimaat, Nationale Agenda Quantum Technologie, 2019
12. Ministerie van Economische Zaken en Klimaat, Strategisch Actieplan AI, 2019
13. Ministeries van Defensie en Economische Zaken & Klimaat, Defensie Industrie Strategie, 2018
14. Ministeries van Defensie, Economische Zaken en Klimaatbeheersing, en Justitie & Veiligheid en Topsector HTSM, Kennis- en Innovatie Agenda Veiligheid, 2019
15. NAVO, AJP-01 ALLIED JOINT DOCTRINE, Edition E Version 1, 2017
16. RAND, *Improving the Cybersecurity of U.S. Air Force Military Systems Throughout Their Life Cycles, 2015*
17. Rid, Thomas, Cyber Warfare will not take place, 2013
18. Smeets, Max, A matter of time: On the transitory nature of Cyberweapons, 2018
19. US Government Accountability Office, Weapon Systems Cybersecurity, DOD Just Beginning to Graple with Scale of Vulnerabilities, 2018
20. Zetter, Kim, Coutdown to Zero Day, 2014

Naast deze open bronnen heeft het onderzoekswerk van TNO van de afgelopen jaren en de gesprekken daarover met mensen uit Defensie en de industrie ook tot inzichten geleid die een plekje in dit document hebben gekregen. Deze mensen blijven hier naamloos, maar onze dank is groot en we brengen deze inzichten graag een stap verder.

Contact
Patrick de Graaf
BUSINESS DIRECTOR CYBERSECURITY
patrick.degraaf@tno.nl

TNO innovation for life

TNO.NL